REMARKS

This Amendment is submitted in response to the office action mailed 2/11/2004. Reconsideration with an eye toward allowance of all claims is respectfully requested. Claims 1-20 have been cancelled and Claims 21-70 added so that Claims 21-70 are pending in this application after entry of this amendment.

Oath/Declaration

The declaration was objected to as allegedly being defective.

A supplemental declaration in compliance with 37 CFR §1.67(a) and §1.52(c)(1) is enclosed herewith.

The Amendments of the Specification

The title of the invention was objected to as allegedly not being descriptive. The title has been amended to more clearly describe the invention.

The disclosure was objected to because of various informalities. The specification has been amended to correct these informalities as suggested by the Examiner.

On page 1, the names of the inventors has been cancelled.

On page 15, line 5, reference number **66** was replaced with **67**. Basis for this amendment is found in FIG. 6A which shows bus **67**.

On page 19, the reference numbers **6A** and **7A** on lines 20 and 21 were replaced with **8A**. Basis for this amendment is found in FIG. 8 showing communications link **8A**.

On page 21, line 2, the reference number **972** was replaced with **971**. Basis for this amendment is found in FIGS. 9A and 9B showing data lines **971**.

On page 21, line 22, a typographical error was corrected.

Accordingly, the amendments do not present new matter and entry is proper.

The Amendments of the Claims

Without admitting the propriety of the rejections in the office action mailed 2/11/04, Applicant has cancelled claims 1-20 without prejudice to reinstate them here or in a related application. New claims 21-70 recite additional features that clarify some of the differences between the cited art and the claims. As the claims have been significantly modified, differences between the cited art and the newly presented substitute claims are addressed.

These new claims largely moot the examiner's rejections based on Goshey et al. (US6205527B1) and Microsoft. However, as the claims now pending still pertain to structures and methods for a self-repairing computer, applicants will address the patentable features relative to the know prior art including to Goshey et al ("Goshey").

Goshey et al (US6205527B1) is directed to an intelligent backup and restoring system and method for implementing the backup and restoring system but it is a system and method with significant limitations that does not solve the problems that are solved by the invention as now claimed. Essentially, Goshey is directed to an external SCSI peripheral storage device that contains a copy of all (if capacity permits) or a user selected portion (if the peripheral storage has a smaller capacity than the computer's hard disk drive) of the computer's hard disk drive. According to Goshey, software generates full or incremental backups of the same files as are present in the computer hard disk so that in the event that the hard disk drive becomes unusable, the peripheral drive can take over operation (with functionality that depends on what subset of files were copied) and attempt to repair the contents of the hard disk drive by restoring files from the peripheral storage device (a storage cartridge) to the hard disk drive. Goshey teaches that the operating system (OS) stored on the peripheral device is the same operating system as on the hard disk drive since it is merely a copy of the other (See Goshey Col. 10, lines 13-33; col. 12, lines 16-18; and col 13, lines 40-46).

Goshey teaches that a version of the backup engine "is charged with performing Virus checking on all files before the copying is performed" so that "in this manner, any detected Viruses are disinfected prior to performing any copying operations" (Col 12, lines 36-40). Unfortunately, this virus checking is and can only be operative if the virus is already known and identified as a virus, and if having identified the virus it can be disinfected. Even using current state of the art anti-viral software available today (but unavailable at the time of Goshey) many known viruses cannot be disinfected or would have caused other problems that cannot be remedied without resort to software or data files that are no longer available on the computer hard disk drive or on the peripheral storage. Therefore, therefore any self-directed automated repair would not be possible without external intervention.

Other prior-art of which applicant is aware, such as reference D1 (EP0978785) cited in a corresponding European Patent Application and cited in an Information Disclosure Statement in this case is directed to a data backup and recovery system and method of limited scope. In particular D1 provides a tape drive that is configured to operate as a bootable device for a PC where as a bootable device it emulates a CD-ROM. In order to provide the intended operation, use of the invention requires "a tape drive and a recent backup of PC data held on tape media" (D1, page 5, lines 34-35). D1 indicates that there are no other changes to the structure of the PC and it is only the tape drive that is modified to accommodate the extended eject button push by a user to place the tape drive into the CD-ROM boot device emulation mode. D1 fails to disclose and structure or method that protects the operating system, application program files, or user data from virus, hackers, or other malicious program code

contamination. If the software or data on the computer is contaminated, attempts to repair the computer software by patching or restoring parts of it that appear to be problematic, rewriting an entire image from the tape drive to the hard disk drive, or any other data recovery may not solve the problem, may solve it only until the computer has been in operation long enough for the virus to cause additional problems, and perhaps worst of all, contaminate the tape backup so that subsequent attempts to recover the software and computer system must usually fail.

Reference D2 (WO95/22794) cited in a corresponding European Patent Application and cited in an Information Disclosure Statement in this case is directed to a system for automatic recovery from software problems that can cause computer failure. The invention achieves this goal at least in part by "means of a user-hidden secondary volume or partition in the computer's permanent storage mechanism, e.g. hard disk" (Page 3, lines 2-4). This secondary volume may store a minimum operating system that will "attempt to automatically fix the detected problem" but may only be limited to get full operation restored by "suggesting possible steps to be taken by the user, in order to fix the problem that resulted in the initial failure. (Page 3, lines 14-17). The error detection and recovery system of the D2 invention "is software-based, and does not rely upon specialized hardware" so D2 clearly neither discloses, suggests, or motivates any need for different architectural computer configuration. It also makes clear that there is a requirement that limits the applicability of the invention, namely, that "[t]he only requirement is that the secondary volume be accessible during the startup process before the main volume is read." (page 8, lines 20-11) It therefore appears to be only applicable at startup and inapplicable during normal operation after startup. D2 does suggest that the secondary volume may be (but does not require) placed on a separate volume because it expects the separate volume to be rarely written to during "normal system operation" and "therefore relatively safe from damage" (page 9, lines 2-4), but D2 has no teaching relative to protection from a virus or other malicious code that can and will exploit any opportunity to infect any volume it can see, especially if that volume is visible during initial boot of the computer system, and particularly operating system files. D2 does not provide any structure or method that guarantees or even attempts to guarantee that once its secondary volume with its operating system are generated that it will not be contaminated by a virus or other malicious software code and either, cause the secondary volume operating system to fail directly, or to infect the primary volume and cause it to fail, or to cause the secondary operating system to infect the primary operating system and cause its failure at a later time. D2 therefore fails to provide any structure or method that alleviates the problems associated with virus, hacker, or other malicious software.

The invention now claimed provide a system, device, and method for the computer to self repair a problem caused by software failure, viral infection, hacker or other malicious code activity. A master template storing content sufficient to restore the operating system, any application programs, and user data stored in a protected and isolated manner in second storage. A repair procedure in the form of a separate operating system and repair program are also stored on second storage (or even some other storage different from the first storage). In the event of a detected problem, the master template and the

repair procedure are used in a manner that neither the master template nor the repair procedure can be contaminated by the contents of the first storage. For example, the repair procedure may provide and use an operating system and program commands which are limited and incapable of executing any content (such as viral or hacker code) on the first storage that might contaminate the processor, the first storage, RAM, the second storage, or any other component of the computer. In one embodiment the repair operating system and application program may only be able to execute copy commands so that no executable code on the first storage can be executed while only the repair operating system and application program are in control. The logical presence of storage, such as disk drives, may also be controlled by the repair procedure to alter the visibility of a drive and to alter the ability and order of the different storage to be booted. These various features provide a computer where a clean system installation is always guaranteed so that a virus and other malicious code free environment can readily be reestablished in the computer. Other embodiments provide for virus free upgrade of the operating system and applications programs as well as backup and restoration of current user files, which even if such user files contain a virus prevents the virus from infecting the protected master template and repair procedure.

In terms of the claims now presented, support is provided in the application as filed in the original specification and claims and in the extensive appendix and drawings. While the attached sheets identify some particular portions of the application that support the new claims, it will be appreciated that the subject matter of the claims is described in various ways throughout the application.

Claim 21, an independent method claim, now requires that the repair be an "automated self-repair of a computer from a software corruption, a virus infection, and a malicious software attack at anytime during operation of the computer including at startup and anytime after startup during use of the computer". Applicant submits that neither Goshey nor any of the other cited prior art teach a repair of this type. As discussed above, Goshey merely makes back-ups of the computer's hard disk drive and cannot self-recover or self-repair the computer from a situation in which a virus, software corruption, or a malicious hacker software attach has damaged a file. Other elements of the claim are more specific as to how the invention accomplishes this and the prior-at cannot..

Claim 21 also requires that the "second storage disposed within the housing of the computer: (i) storing a master template and (ii) a repair procedure that are completely isolated and protected from alteration by viral infection and malicious code from untrusted sources". Applicant submits that neither Goshey nor any other cited reference teach both "(i) storing a master template and (ii) a repair procedure" and/or that they are "completely isolated and protected from alteration by viral infection and malicious code from untrusted sources". Goshey does not have a master template that is isolated and protected in the manner claimed. Even if the backup copy of Goshey were to be interpreted as a master template (and we argue that it should not be) then it clearly is not protected as it is merely a copy of the hard disk drive, is connected to the harddrive via the processor or other standard computer components, and any entity within the computer would have read/write access to the peripheral storage

which in one instance is described as running in the background while normal operation occurs within the computer.

Claim 21 also requires that the "repair procedure being stored on logically different and separately addressable and isolated storage from each other and from the first storage, the second storage not capable of being exposed to the an untrusted data or program source". Again, Goshy fails to disclose, teach, suggest, or motivate any need for this element. Goshey repair procedure is merely maintaining an external storage that copies the contents of the computer hard disk drive and uses the copied contents to restore the hard disk drive in the event it fails. The repair procedure itself is stored on the hard disk before the first backup to the peripheral storage and no attempt is ever made at maintaining them in isolation. Neither does Goshey describe structure the second storage (peripheral storage) is not capable of being exposed to the an untrusted data or program source (other than unplugging the peripheral) and yet would still provide automated self repair.

Claim 21 also requires that in the normal mode, "the first storage is physically present within the housing of the computer and able to support read and write operations, and the second storage is physically present within the housing of the computer but logically hidden and unable to support a write operation communication from the first storage, the first processor, the first random access memory, or the first BIOS memory; and (b) in the repair mode, the first storage is physically present in the computer and able to support read and write operations, and the second storage is physically present in the computer and logically visible and able to have only predetermined communication controlled by the repair procedure with the first storage, the predetermined communication being permitted only through a trusted processor and memory executing a repair procedure that are known to be virus and malicious code free". Applicant submits that neither Goshey nor other cited art teach nor suggest these features.

The peripheral or second storage device of Goshey is described as being an external SCSI storage device and it is illustrated as such in FIG. 1A and neither "physically present within the housing of the computer but logically hidden and unable to support a write operation communication from the first storage" when in the normal mode, nor "physically present in the computer and logically visible and able to have only predetermined communication controlled by the repair procedure with the first storage, the predetermined communication being permitted only through a trusted processor and memory executing a repair procedure that are known to be virus and malicious code free". In particular, Goshey fails to teach or suggest performing the repair operations through "a trusted processor and memory executing a repair procedure that are known to be virus and malicious code free."

Finally, Claim 21 requires that the repairing includes "generating the executable computer program instructions on the first storage using the repair procedure to copy at least a portion of the master template to the first storage through a trusted processor and memory executing a repair procedure that are known to be virus and malicious code free". Applicant submits that the back-up of Goshey is not a master template, and that Goshey fails to teach or suggest copying ... to the first storage

through a trusted processor and memory executing a repair procedure that are known to be virus and malicious code free." Not only does Goshey and the other cited art fail to teach or suggest the individual elements of Claim 21, they also fail to teach or in any way suggest the overall methodology, function, or structure recited in the claim. While several basis for overcoming a rejection over Goshey and the other art have been recited here, it will be appreciated than any one of the reasons recited is alone sufficient to support patentability of the claims. The prior-art systems and methods do not provide a method for automated self-repair of a computer from a software corruption, a virus infection, and a malicious software attack at anytime during operation of the computer including at startup and anytime after startup during use of the computer at least because they do not provide and maintain the isolation of the master template and the repair procedure from recontamination during a repair.

Claim 22, imposes the further requirement that the "trusted processor and memory are the first processor, first random access memory, and first BIOS memory that have been cleared of any executable virus or malicious code by the repair procedure prior to permitting any communication with the second storage". As compared to the prior-art, for example, where the tape drives or other peripheral storage devices are used, the storage media is not isolated from infection and is subject to being overwritten by virally infected code because no steps are taken to clear the processor, RAM, and BIOS so that they have a known content and can be trusted not to re-contaminate the computer. Even where attempts are taken to prevent copying of "known" viruses, there is no ability to prevent contamination from unknown viruses or to self-repair when a bad file coul dnot be repaired. Furthermore, there is no suggestion in the cited art that the operating system used during a repair is limited in a way that prevents it from executing any content of the storage device on which the repair (or reload) is being attempted. Goshey describes the backup operating system as being the same as the operating system on the computer's hard disk drive, and only suggests that a smaller portion of it be used if there is a capacity limit. It is clear from the description that the operating system components on the backup are consistent with and provide support for code resident on the first storage so that Goshey cannot "prevents it from executing any content of the storage device on which the repair (or reload) is being attempted".

Claim 23, recites an alternative embodiment, where a second computing environment is used and provides that "the trusted processor and memory are a second processor, a second random access memory, and a second BIOS memory that have been cleared of any executable virus or malicious code by the repair procedure prior to permitting any communication with the second storage. Neither Goshey nor other cited art disclose a second computing environment established in the computer having this structure or function.

Claim 24, requires "an integrated second computing system operating concurrently with the computing system and having a second processor and a second random access memory coupled with the second processor" and then particular method steps performed by the (first) computer and the second computing system. We do not repeat all the steps here but rather refer the examiner to the claim

itself. Neither Goshey nor other cited art disclose a second computing environment established in the computer having this structure or function

Other of the dependent claims recite additional differences between the invention and the cited art. The examiner is respectfully referred to the claims and the claim language is not repeated here.

Claims 63 and 64 are independent computer apparatus claims which recite similar though not identical elements to those in the independent method claim 21. At least the same arguments pertain to the structures of claims 63 and 64 (and their dependent elements) that have been argued relative to claim 21.

Applicant has utilized the written description in the drawings and substantial appendix to present in the claims and no new subject matter has been added that is not in the application as filed. Upon the indication of allowable subject matter, the examiner is invited to request amendment of the specification to add description from the appendix into the specification as may be required.

Applicants herewith also submit a replacement Declaration and request a Corrected Filing Receipt be issued reflecting the title change to the specification.

CONCLUSION

With these amendments and remarks, applicant trusts that the 35 USC 102 and 35 USC 103 rejections will be withdrawn. Applicant request the opportunity of an interview and demonstration if the examiner believes that the claims as now presented fail to identify patentable subject matter.

Respectfully submitted,
DORSEY & WHITNEY LLP

By _____
R. Michael Ananian, Reg. No. 35,050

Customer No. 32940
DORSEY & WHITNEY LLP
Four Embarcadero Center - Suite 3400
San Francisco, California 94111-4187
Tel.: (415) 781-1989
Fax: (415) 398-3249
PA-1073067V1